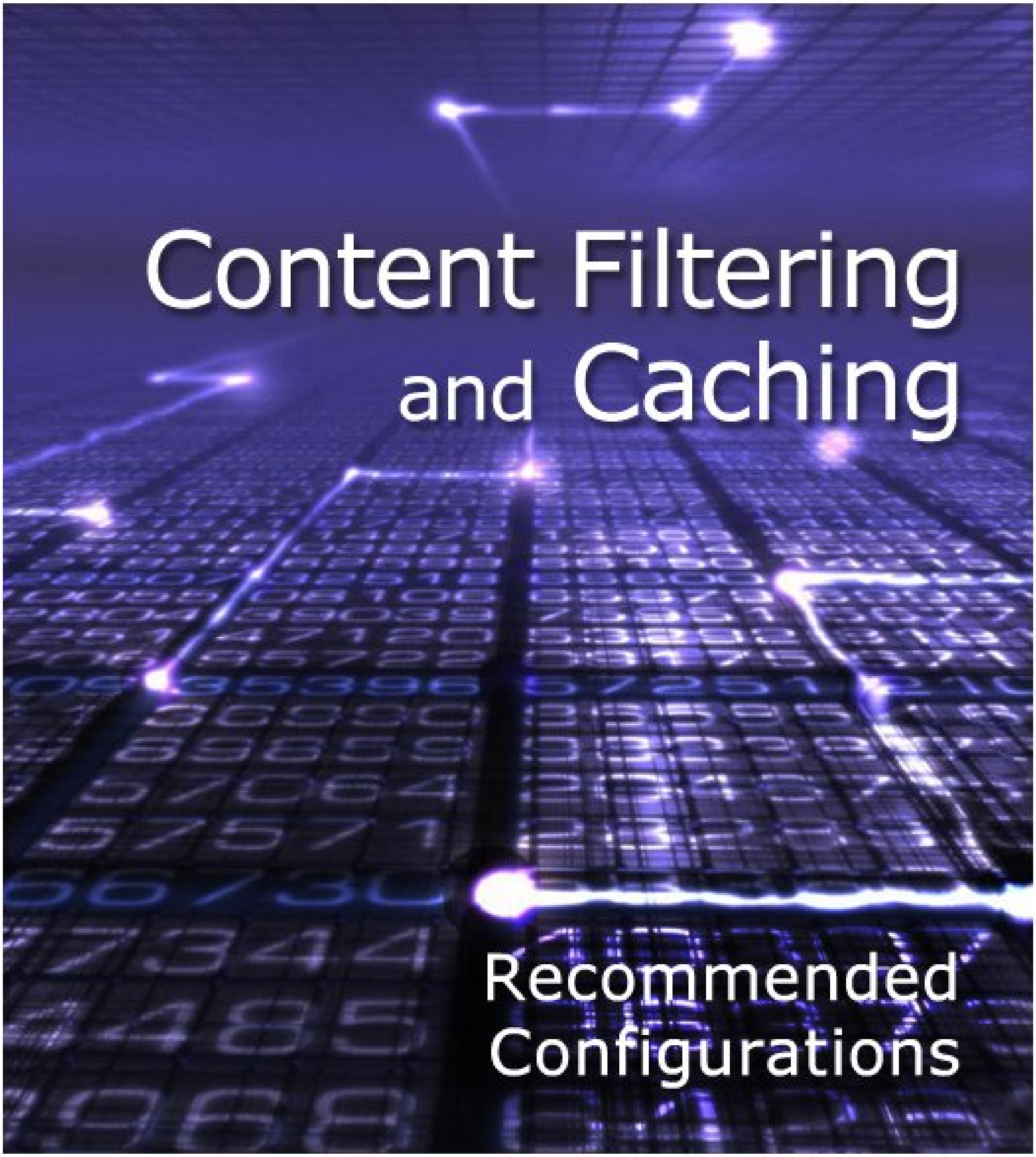
PEM SOLUTIONS
PEARSON EDUCATIONAL MEASUREMENT SOLUTIONS



Content Filtering and Caching

Recommended Configurations

PEARSON

Published August 28, 2007

Overview

Pearson PEM tests the most common content filtering and caching solutions used in conjunction with PEMSolutions. The primary focus of this testing is to develop a set of configuration guidelines for districts/schools to use in preparing for implementation of online testing using PEMSolutions.

(Note: This document is not intended to be an endorsement of any particular content filtering solution.)

PEMSolutions consists of two primary applications:

1. The administrative website, which is accessed via a web browser by authorized test administrators.
2. TestNav™, which is a locally installed Java application used for delivering tests to students.

Proxy Server Configuration

Proxy Environments

Many customer networks use proxy servers in their network environments. Proxy servers are placed between client nodes and the Internet and are used to forward requests from internal nodes to the Internet. Proxy servers may also perform some or all of the following functions:

- **Protocol Filtering** to control which protocols are forwarded to the Internet
- **User Authentication** to control who can access the Internet
- **Machine Authentication** to control which machines can access the Internet
- **Content Filtering** to control which Internet content users can access
- **Content Caching** to speed access for frequently visited sites

In order for an application to access the Internet in a proxy server environment, the application must know the hostname and port number of the proxy server. Once the application is made aware of the proxy server, all requests for network services are sent to the proxy server for processing. The proxy server receives the incoming requests and must determine what to do with them. If all of the functions listed above have been implemented, the proxy server will:

1. Verify that the protocol of the request is serviceable (i.e., ICMP, UDP, etc. may be blocked by the proxy server).
2. Ask the user to authenticate that the proxy server does not already recognize him/her as being logged in.
3. Verify that the source address of the request is on the list of allowed machines.
4. Verify that the requested network object is not banned by a filter. (Most proxy server vendors provide lists of sites organized by category that administrators can decide to block or allow.)
5. Check the proxy server's local disk to see whether the requested object exists in cache. (If the object is in cache, the proxy server will send it directly to the requestor without getting it from the Internet.)

Assuming that the request passes all of the above steps, the proxy server then stores a record of the request in memory and issues its own request for the same object out to the Internet. When the reply returns to the proxy server, the server matches the reply to the original request stored in memory and forwards the reply to the original requestor.

Configuring a Proxy Environment for TestNav

- **Protocols:** TestNav uses the same protocol to communicate on the Internet as a web browser: TCP/http. Proxy servers and firewalls must be configured to allow http on port 80 to the Internet.

> If your school is using **Symantec Web Security** as an Internet content filter AND has it configured to require individual user authentication, follow these steps for launching TestNav:
>
> 1. Open an industry-standard browser.
> 2. Login to Symantec Web Security.
> 3. Keep the browser open.
> 4. Launch TestNav.

- **User Authentication:** TestNav is capable of authenticating with proxy servers that adhere to the HTTP 1.0 specification. If TestNav is being run from behind a proxy server that requires authentication, it is recommended that testing be performed to ensure that TestNav can authenticate properly. If authentication is not successful via TestNav, it is recommended to have examinees log in using a web browser prior to launching TestNav. In this situation, the proxy server administrator should make sure that the timeout period for a user’s authentication is long enough that they will not be asked to log in again for the duration of the test.
- **Machine Authentication:** All machines running TestNav must be recognized by the proxy server as valid clients.
- **Content Filtering:** The following URLs must be allowed through any content filters that have been implemented:

etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com

- **Content Caching:** Web caching can greatly reduce the amount of bandwidth required for testing as well as increase the speed of test item downloads. It is recommended that caching be enabled on proxy servers that support it.
- **Name Resolution:** TestNav uses DNS to resolve the above hostnames to IP addresses when communicating. Clients must be able to query DNS to resolve the hostnames listed above If there are problems with DNS functioning correctly, a local host’s file may be used with the following entries:

etest.pearson.com	**206.17.160.33**
www8.etest.pearson.com	**206.17.160.38**
www9.etest.pearson.com	**206.17.160.37**
launcher.etest.pearson.com	**206.17.160.37**

Configuring TestNav for a Proxy Environment

For the Proctor Caching Server to receive requests for test content, TestNav must be configured to use the Proctor Caching Server as a proxy server. **TestNav typically is configured during installation to use Proctor Caching Server as a proxy server.** If it was not configured during installation, follow these steps:

1. Using a text editor, such as notepad, open the “proxysettings.properties” file located in the same directory in which TestNav is installed.
2. On the “Proxy_Host=” line, enter the IP address of the Proctor Caching Server.
3. On the “Proxy_Port=” line, enter 4480.
4. The “Proxy_Auth_Required=” line can be left blank.

Caching

Caching refers to the storage of web content by a proxy server. This stored content is used to satisfy client requests directly from the proxy server’s cache.

> Test items retrieved by the TestNav application are fully cacheable. The administrative website, however, uses SSL to encrypt communications, which prevents the content from being cached.

Benefits of Caching

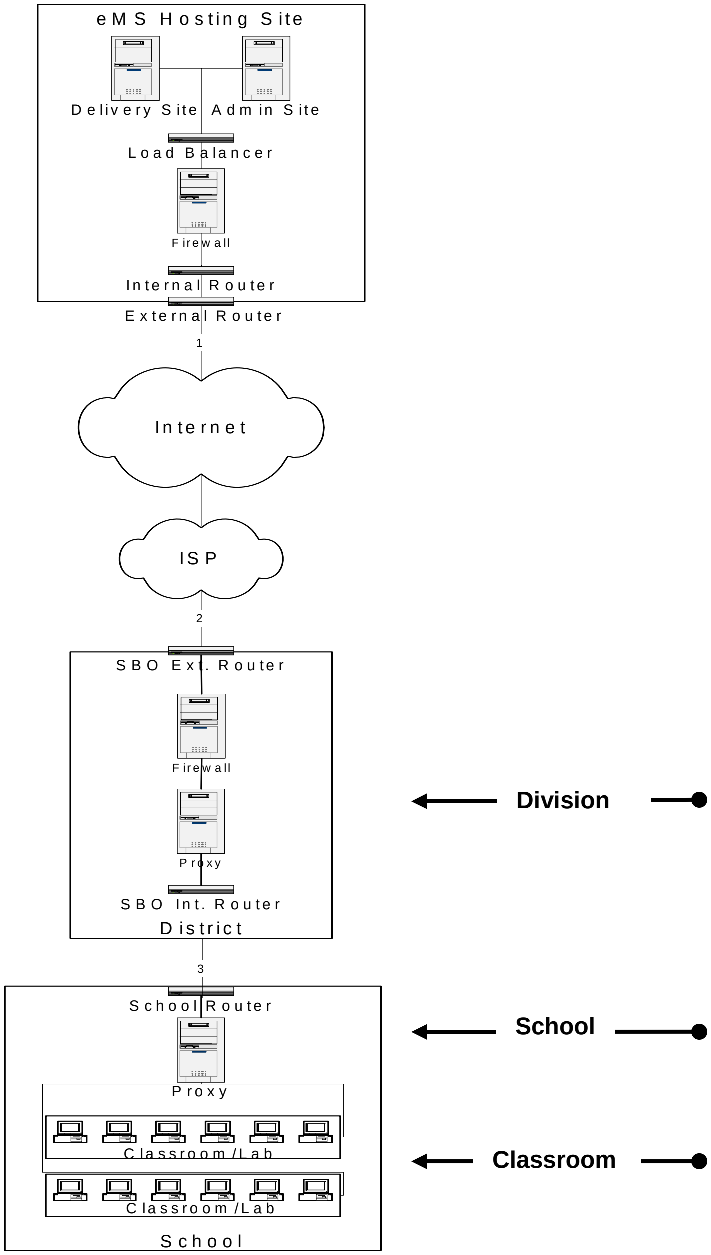
Effective caching reduces the number of requests that must be sent from the testing environment across the Internet to the web server. A description of the standard HTTP cache algorithm is provided in Figure 2 later in this document. The reduction of requests provides the following benefits:

- **Reduced bandwidth requirements for the testing environment.** Once the proxy server’s cache has been populated with the cacheable content (test items), the proxy server should respond directly to all future requests for any items in its cache. This will conserve bandwidth to the Internet by not downloading identical content for multiple users. In a cached environment, bandwidth demand can be reduced by as much as (N-1)*T, where N is the number of examinees and T is the size of the test being administered. Caching at the school or school district level will lower the bandwidth requirements for testing.
- **Faster test downloads.** Once a cache server has been loaded with the necessary items for a test administration, the local proxy server should respond directly to all client requests for test items. This results in removing the primary network bottlenecks and allows the test items to be served from a source much closer to the client.

How to Implement Caching

The diagram below depicts the three likely points at which caching can be implemented. Caching can be implemented on proxy servers located at the district, school, or classroom levels of the network hierarchy. In addition, if proxy servers exist at more than one of these levels, they can be used in conjunction to further increase the benefits of caching.

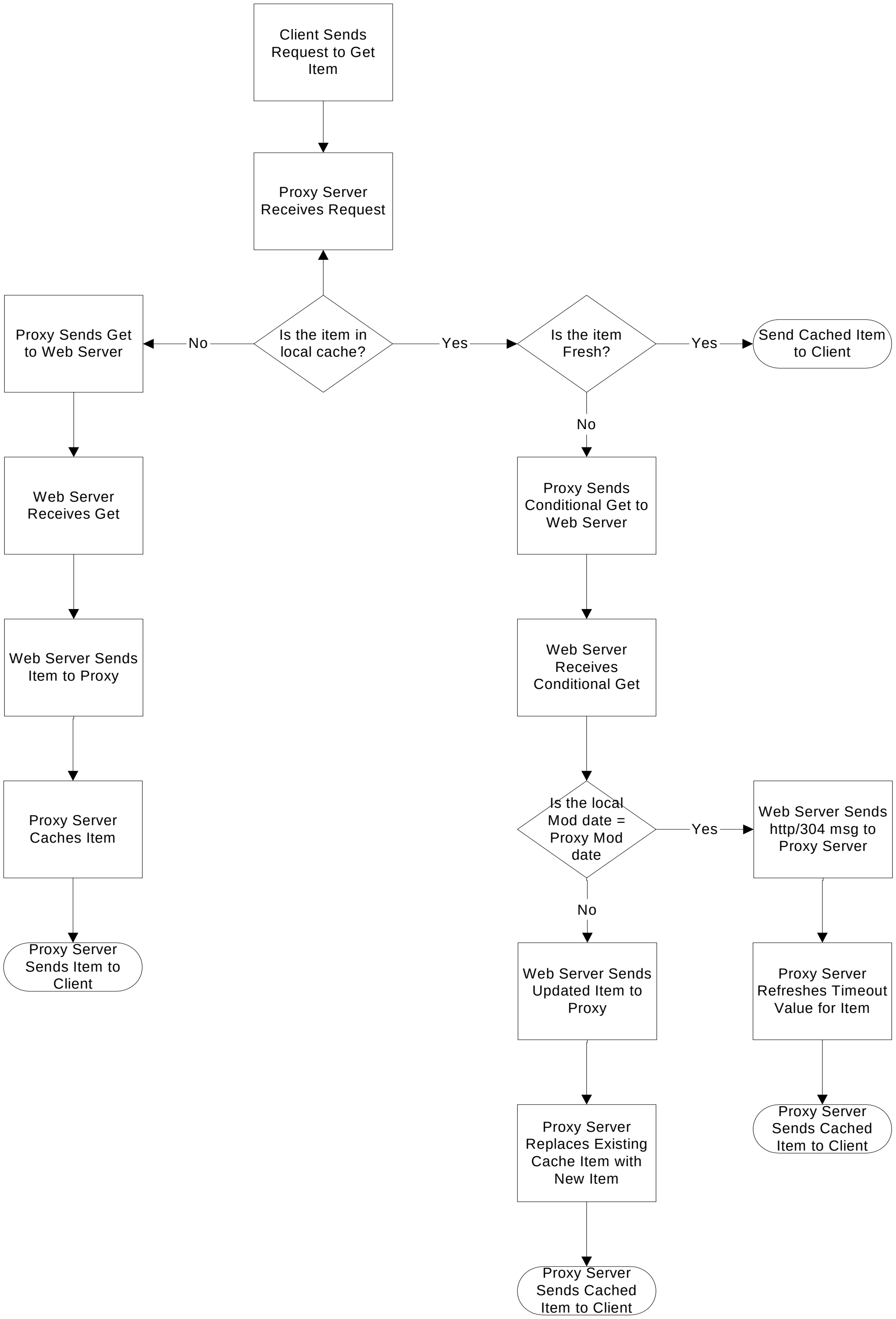
Figure 1 – Caching Implementation Points



Cache Priming

To get the maximum benefits from the caching of test items, the cache should be populated prior to students taking the test. This can be accomplished by, for example, having a single student log into a test session five minutes before the rest of the examinees. The flow chart below shows the steps of the client request process in a cached environment.

Figure 2 – Standard HTTP Cache Algorithm


Client Sends Request to Get Item
Proxy Server Receives Request
Is the item in local cache?
No
Yes
Proxy Sends Get to Web Server
Is the item Fresh?
Yes
Send Cached Item to Client
No
Web Server Receives Get
Proxy Sends Conditional Get to Web Server
Web Server Sends Item to Proxy
Web Server Receives Conditional Get
Proxy Server Caches Item
Is the local Mod date = Proxy Mod date
Yes
Web Server Sends http/304 msg to Proxy Server
No
Proxy Server Sends Item to Client
Web Server Sends Updated Item to Proxy
Proxy Server Refreshes Timeout Value for Item
Proxy Server Replaces Existing Cache Item with New Item
Proxy Server Sends Cached Item to Client
Proxy Server Sends Cached Item to Client

Configuration Guidelines for Filtering Software

This document provides both generic and product-specific configuration guidelines for filtering software. The generic guidelines apply to any content-filtering solution for a district implementing online testing. In addition, guidelines for specific filtering software are presented following the generic guidelines. You can choose whether to use the generic or the appropriate product-specific guideline.

Generic Configuration Guidelines

Based on the results of PEM's testing, the following generic recommendations apply to any content-filtering solution for a district implementing online testing:

1. **Add the following URLs to your content filtering solution's "local override" database:**

etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com

   Each of these URLs is used by PEMSolutions. In most cases, adding these URLs to your filtering solution's "local override" database will prevent any further interrogation of the content from these sites. In other words, these sites will be fully "trusted" or "open" to your users.

   In most filtering solutions, adding these URLs to your "local override" database will provide a relatively minor performance improvement for online testing. This performance improvement is a result of the URLs not being checked against your content filtering software's "banned sites" database (which can be quite large).

2. **Make use of your filtering solution's "bandwidth throttling" capabilities (if available).**

   Many filtering solutions have the ability to manage access to "high bandwidth" Internet content, such as streaming video and MP3 files. *If it is available and appropriate in your environment*, use of this feature during testing is recommended. This would allow for tighter control over bandwidth use and may help preserve your Internet bandwidth for delivery of online tests. Use of this feature, however, is *not a requirement* for implementing online testing.

3. **Follow your content filtering software solution's recommended hardware recommendations.**

   Because of the wide range of hardware requirements for content-filtering software, PEM cannot make specific hardware configuration recommendations. However, it is important to recognize the important role your content filtering solution can play in impacting the performance of your Internet connection. Please read your content filtering solution provider's hardware recommendations carefully.

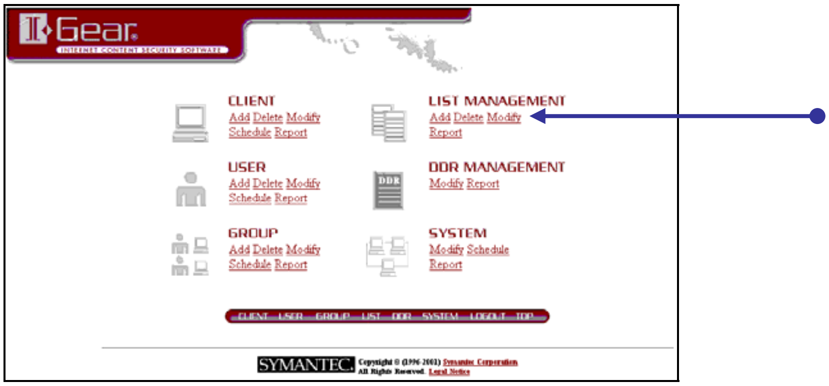
4. **Enable content caching for Internet content.**

   Enabling content caching on the proxy server will reduce the amount of Internet traffic required for testing. The amount of disk and memory allocated to caching on a given proxy server depends on the total amount of requests it is serving. In general, the more disk and memory that can be allocated, the better the performance.

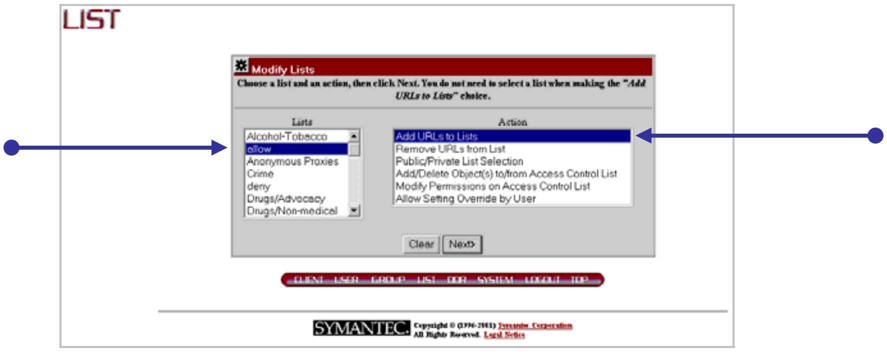
Symantec Web Security (I-Gear) Configuration Guidelines

URL Access

1. On the Admin screen, select LIST MANAGEMENT / Modify.



2. On the Modify Lists screen, select Allow in the Lists field, then select Add URL's to Lists in the Action field. Click **Next**.

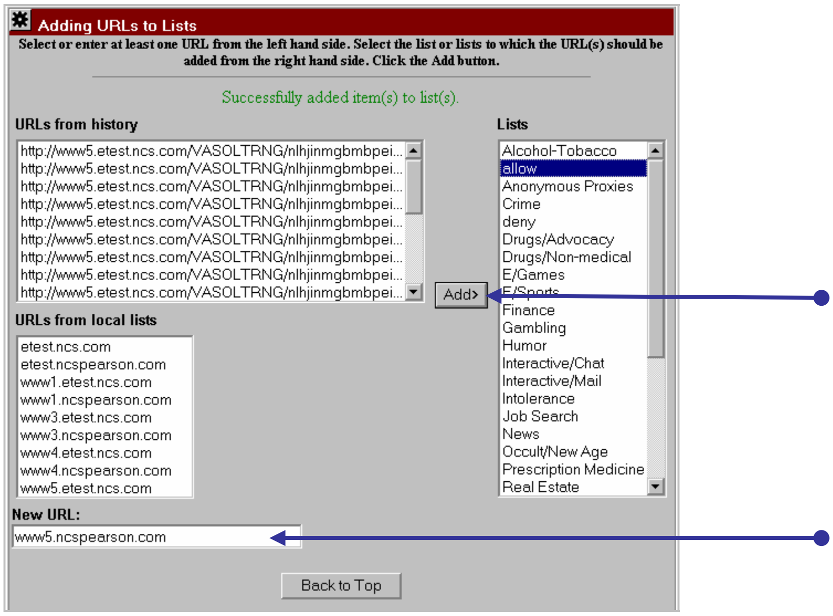


Choose a list and an action, then click Next. You do not need to select a list when making the "*Add URLs to Lists*" choice.

Lists
Alcohol-Tobacco
allow
Anonymous Proxies
Crime
deny
Drugs/Advocacy
Drugs/Non-medical
Action
Add URLs to Lists
Remove URLs from List
Public/Private List Selection
Add/Delete Object(s) to/from Access Control List
Modify Permissions on Access Control List
Allow Setting Override by User
Clear
Next>
CLIENT USER GROUP LIST DDR SYSTEM LOGOUT TOP
SYMANTEC.
Copyright © (1996-2001) Symantec Corporation
All Rights Reserved. Legal Notice

3. On the Add URLs to List screen, add the following URLs by entering each URL in the New URL field. Click **Add.**

etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com



Adding URLs to Lists

Select or enter at least one URL from the left hand side. Select the list or lists to which the URL(s) should be added from the right hand side. Click the Add button.

Successfully added item(s) to list(s).

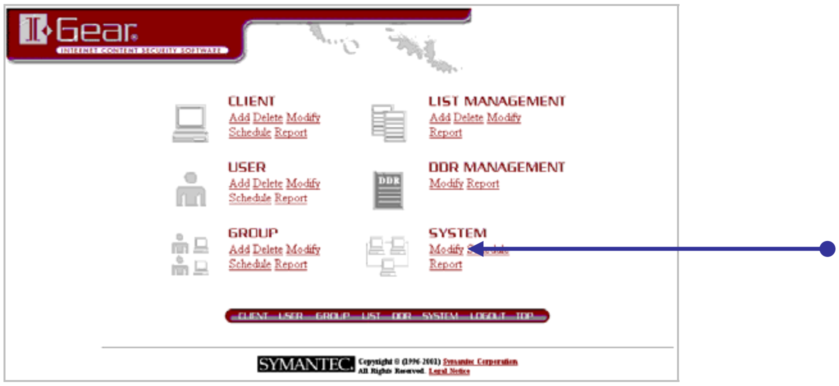
Lists: allow

New URL: www5.ncspearson.com

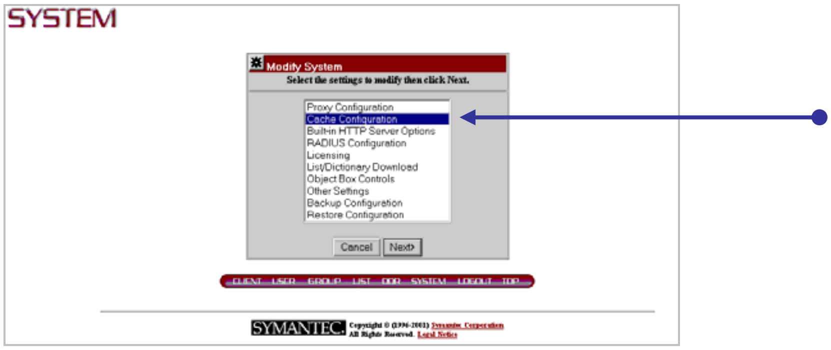
URLs from history
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
http://www5.etest.ncs.com/VASOLTRNG/nlhjinmgbmbpei...
Add>
URLs from local lists
etest.ncs.com
etest.ncspearson.com
www1.etest.ncs.com
www1.ncspearson.com
www3.etest.ncs.com
www3.ncspearson.com
www4.etest.ncs.com
www4.ncspearson.com
www5.etest.ncs.com
Lists
Alcohol-Tobacco
allow
Anonymous Proxies
Crime
deny
Drugs/Advocacy
Drugs/Non-medical
E/Games
E/Sports
Finance
Gambling
Humor
Interactive/Chat
Interactive/Mail
Intolerance
Job Search
News
Occult/New Age
Prescription Medicine
Real Estate
Back to Top

Cache Settings

1. On the Main Admin screen, select SYSTEM / Modify.



2. On the Modify System screen, select Cache Configuration. Then click **Next**.



SYSTEM

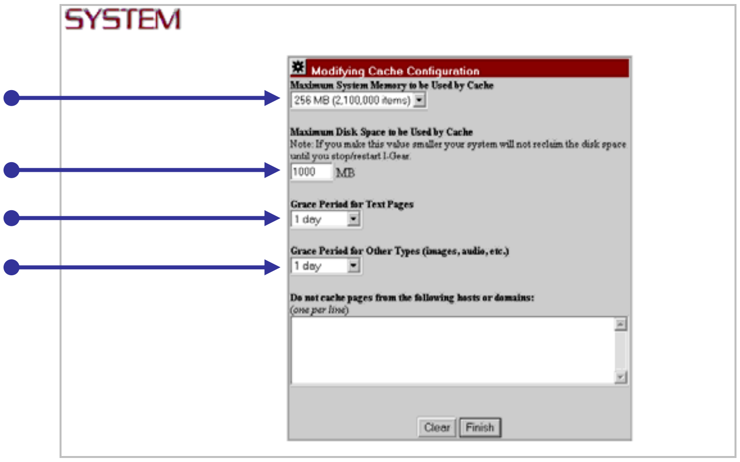
Modify System

Select the settings to modify then click Next.

Cache Configuration

3. On the Modifying Cache Configuration screen, our recommended settings for the displayed fields are as follows:

- In the Maximum System Memory to Be Used By Cache field, we recommend that cache is given as much memory as feasible. TestNav will not consume more than a few hundred items, but it is assumed that other web traffic will be cached at the same time.
- In the Maximum Disk Space to be Used by Cache field, we recommend that the maximum disk space be set as high as feasible, given the specific server and web surfing environment. Symantec recommends a minimum setting of 100MB. (This setting controls how much disk space I-Gear will consume with cached items.)
- In the Grace Period for Text Pages field, our recommended setting is 1 day. (This setting controls how often the cache content is verified as current.)
- In the Grace Period for Other Types field, our recommended setting is 1 day. (This setting controls how often the cache content is verified as current.)



Modifying Cache Configuration

Maximum System Memory to be Used by Cache: 256 MB (2,100,000 items)

Maximum Disk Space to be Used by Cache
Note: If you make this value smaller your system will not reclaim the disk space until you stop/restart I-Gear.
1000 MB

Grace Period for Text Pages: 1 day

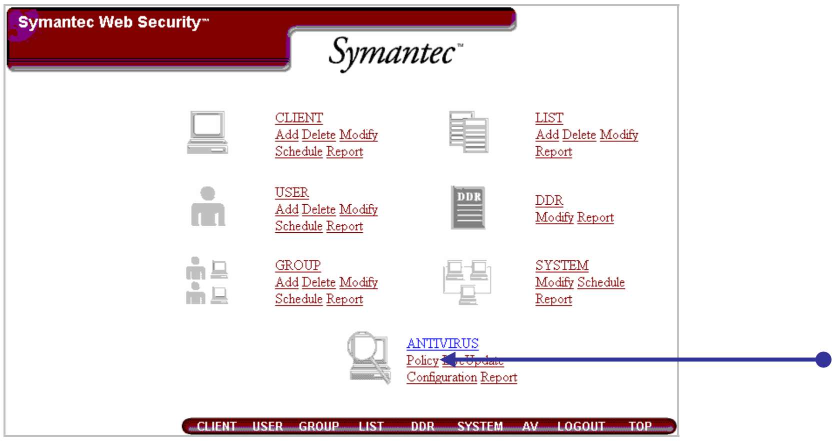
Grace Period for Other Types (images, audio, etc.): 1 day

Do not cache pages from the following hosts or domains:
(one per line)

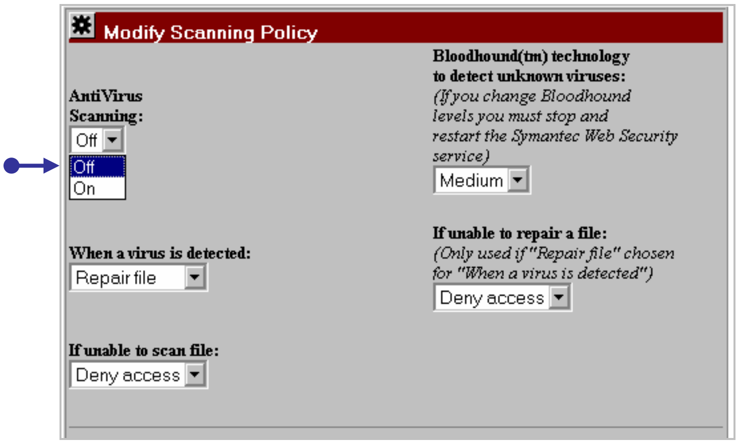
AntiVirus Settings

The AntiVirus scanning engine integrated with Symantec Web Security has a conflict with TestNav because of the “please wait” messages it sends clients while it is scanning Internet content. Due to this conflict, the antivirus scanning engine must be disabled during testing periods. The following steps illustrate how to disable the antivirus engine.

1. On the Admin page, select ANTIVIRUS / Policy.



2. On the AntiVirus Policy Screen, select OFF in the AntiVirus Scanning field.



Modify Scanning Policy

AntiVirus Scanning: Off
Off
On

Bloodhound(tm) technology to detect unknown viruses: *(If you change Bloodhound levels you must stop and restart the Symantec Web Security service)* Medium

When a virus is detected: Repair file

If unable to repair a file: *(Only used if "Repair file" chosen for "When a virus is detected")* Deny access

If unable to scan file: Deny access

3. Click **Finish** to enter changes.

Cyber Patrol/Microsoft ISA Server Configuration Guidelines

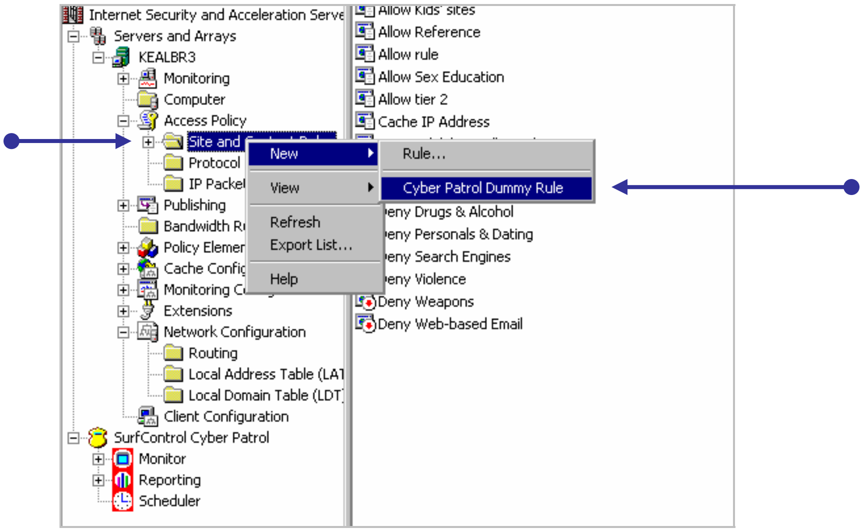
Create an Access Policy

The most efficient way to allow access to these PEMSolutions sites with CyberPatrol/ISA is to create an access policy that allows access for all clients to ***.etest.pearson.com**. This access policy will allow access to the following URLs by creating a new Cyber Patrol Dummy Rule.

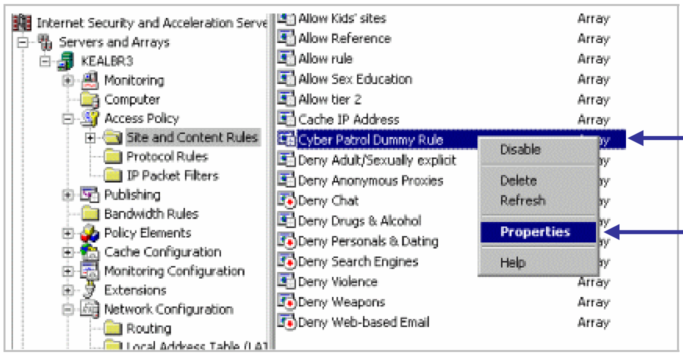
etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com

In the ISA Server Management Console, create a new Cyber Patrol Dummy Rule by:

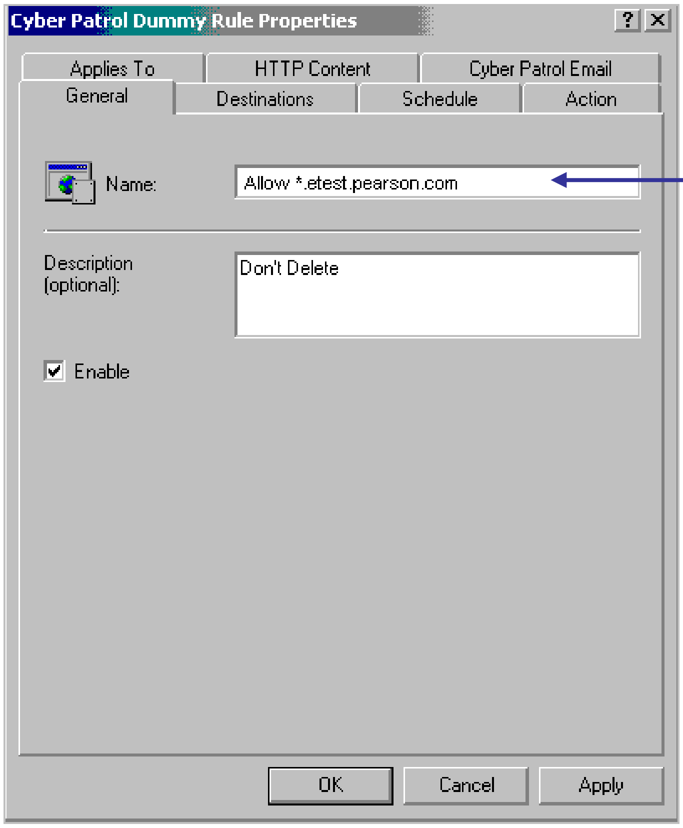
1. Right clicking on the Site and Content Rules folder. Select New / Cyber Patrol Dummy Rule.



2. Select Cyber Patrol Dummy Rules / Properties.



3. On the General tab, enter **Allow *.etest.pearson.com** in the Name field.

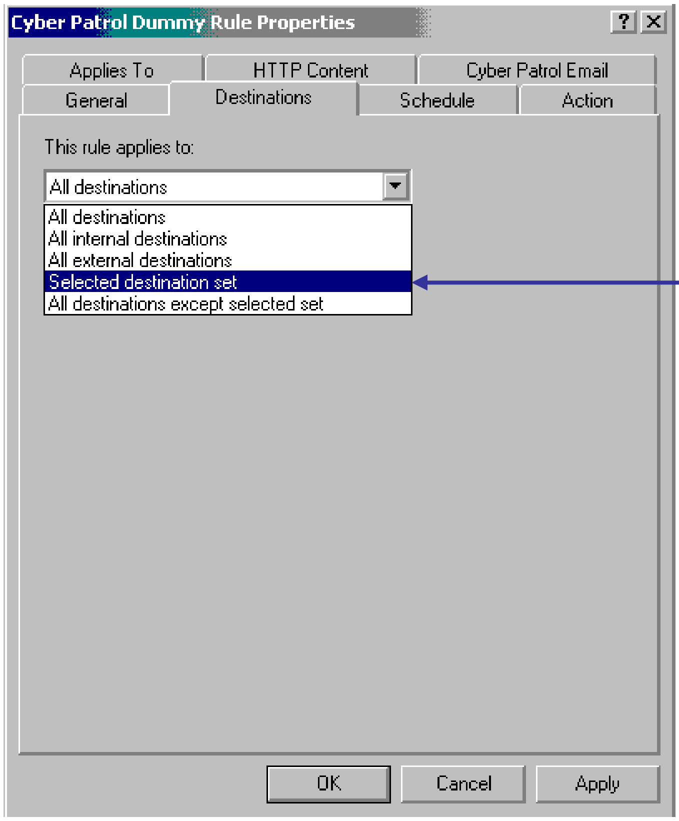


Name: Allow *.etest.pearson.com

Description (optional): Don't Delete

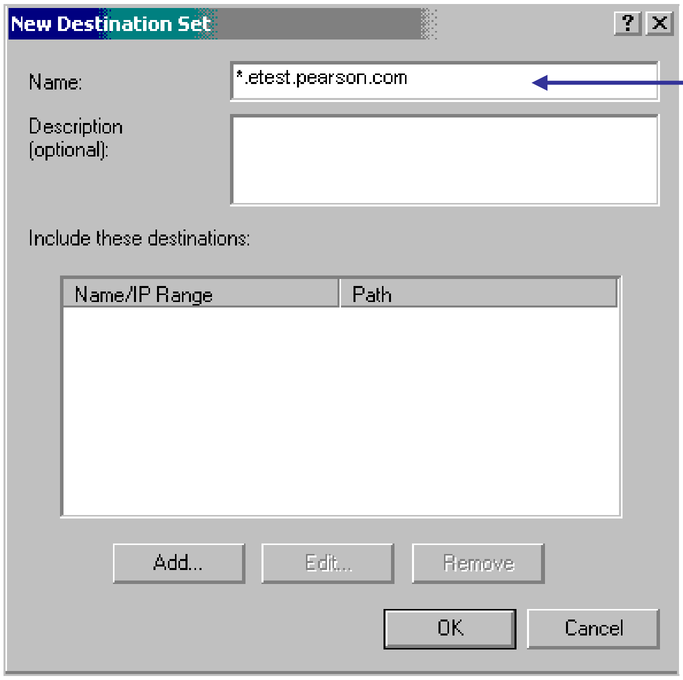
☑ Enable

4. Select the Destinations tab, then select Selected Destination Set in the This Rule Applies To field. Click **Apply**.



This rule applies to: Selected destination set

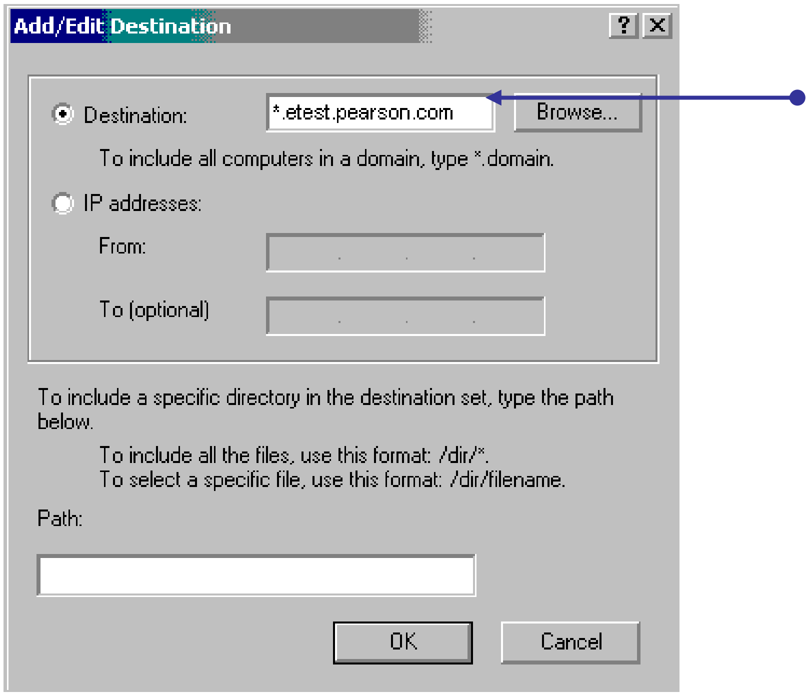
5. In the Name field, enter ***.etest.pearson.com** then click **OK**.



Name: *.etest.pearson.com

Description (optional):

6. In the Destination field, enter ***.etest.pearson.com**, then click **OK**.



Add/Edit Destination

● Destination: *.etest.pearson.com Browse...

To include all computers in a domain, type *.domain.

○ IP addresses:

From:

To (optional)

To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.
To select a specific file, use this format: /dir/filename.

Path:

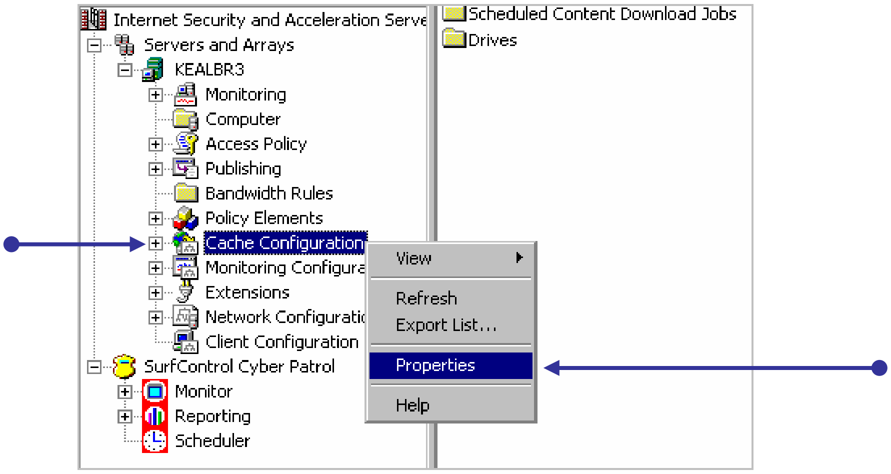
OK Cancel

7. Continue clicking **OK** until all dialogue boxes are closed.

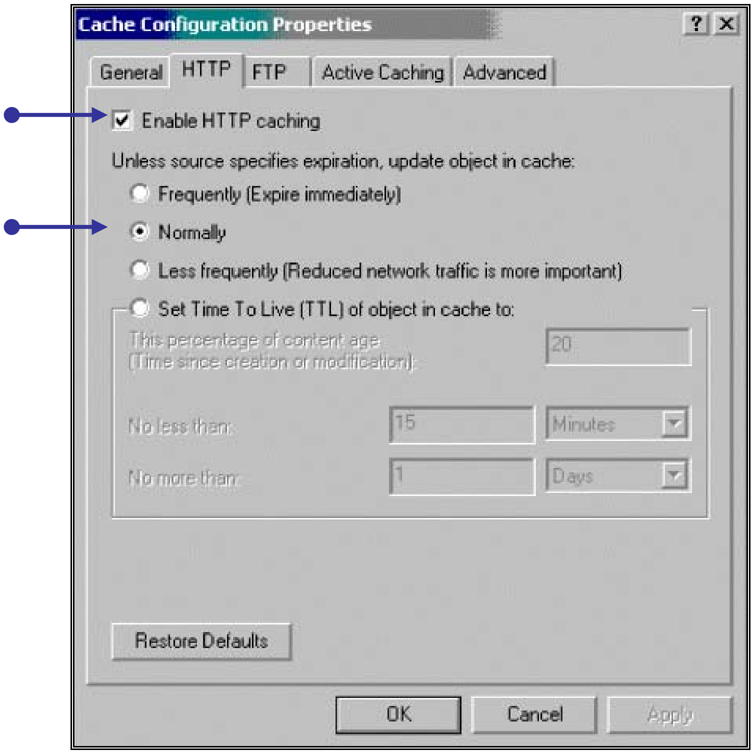
Enable HTTP Caching within Microsoft ISA Server

Enabling HTTP caching will reduce the amount of Internet bandwidth required for electronic testing. To configure HTTP caching:

1. On the ISA Server Management Console, right click on Cache Configuration, then select Properties.



2. Select the HTTP tab and enable Enable HTTP caching by placing a check in the check box. Set the expiration to Normally.



☑ Enable HTTP caching

Unless source specifies expiration, update object in cache:

○ Frequently (Expire immediately)

● Normally

○ Less frequently (Reduced network traffic is more important)

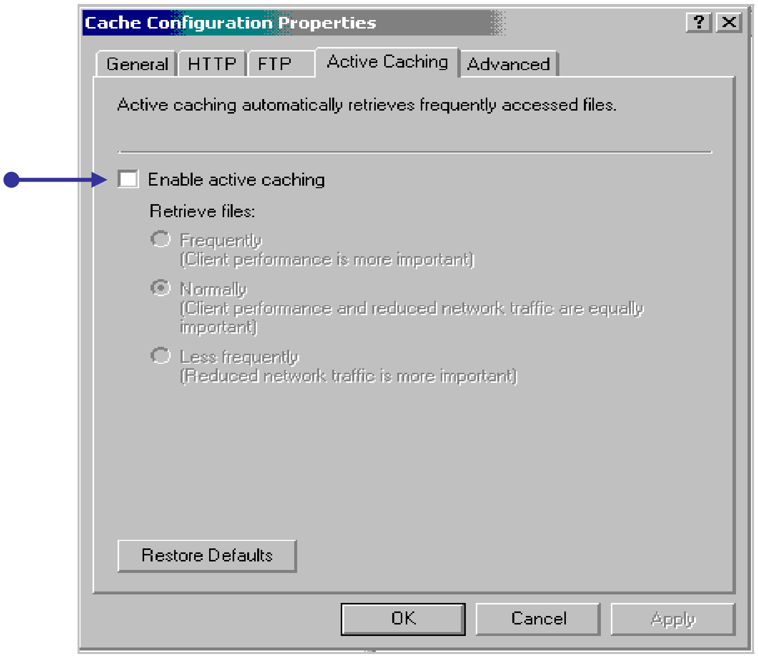
○ Set Time To Live (TTL) of object in cache to:

This percentage of content age (Time since creation or modification): 20

No less than: 15 Minutes

No more than: 1 Days

3. Select the Active Caching tab and disable Enable Active Caching by ***removing*** the check from the Enable Active Caching check box.



Active caching automatically retrieves frequently accessed files.

□ Enable active caching

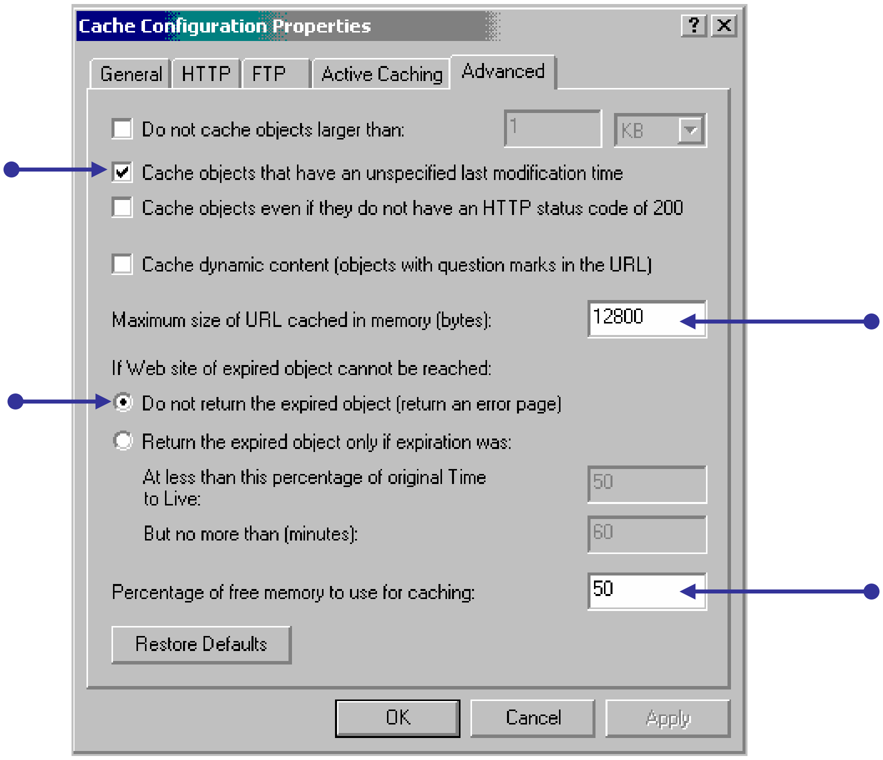
Retrieve files:

○ Frequently (Client performance is more important)

● Normally (Client performance and reduced network traffic are equally important)

○ Less frequently (Reduced network traffic is more important)

4. Select the Advanced tab and configure the options as shown below.



Cache Configuration Properties

□ Do not cache objects larger than: 1 KB

☑ Cache objects that have an unspecified last modification time

□ Cache objects even if they do not have an HTTP status code of 200

□ Cache dynamic content (objects with question marks in the URL)

Maximum size of URL cached in memory (bytes): 12800

If Web site of expired object cannot be reached:

● Do not return the expired object (return an error page)

○ Return the expired object only if expiration was:

At less than this percentage of original Time to Live: 50

But no more than (minutes): 60

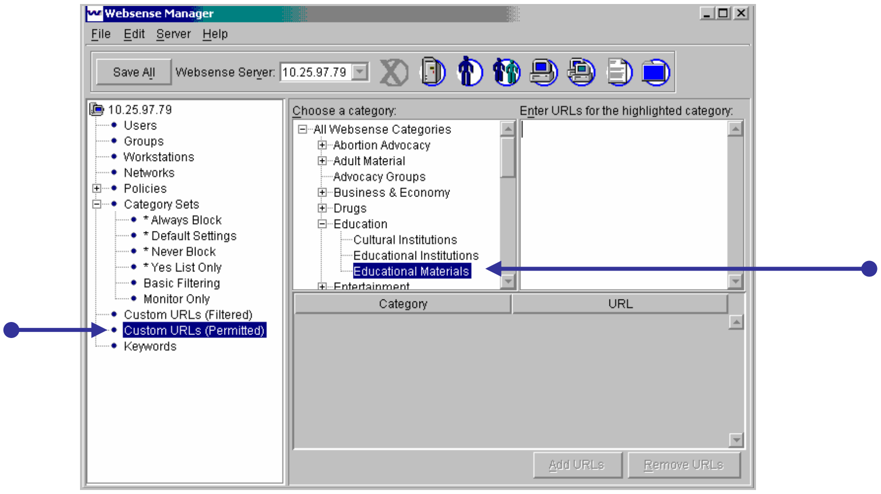
Percentage of free memory to use for caching: 50

5. Click **OK** to implement changes.

Websense / Microsoft ISA Server Configuration Guidelines

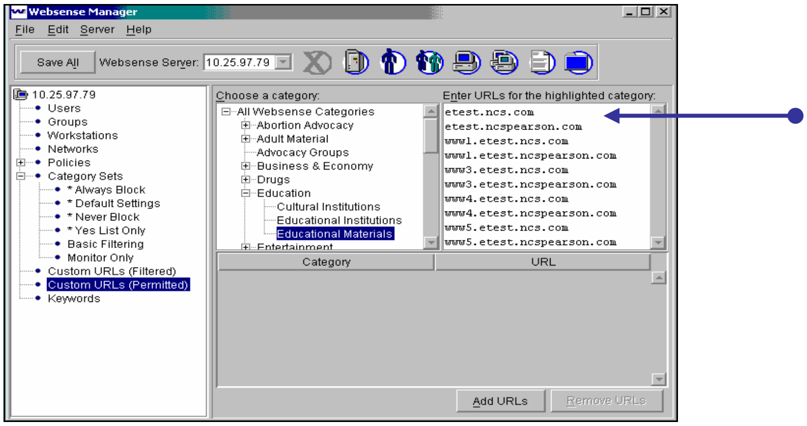
URL Access

1. On the Websense Manager screen, select Custom URLs (Permitted), then select the Educational Materials category.



2. Enter the following URLs in the Enter URLs for the Highlighted Category field

etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com



Enter URLs for the highlighted category:

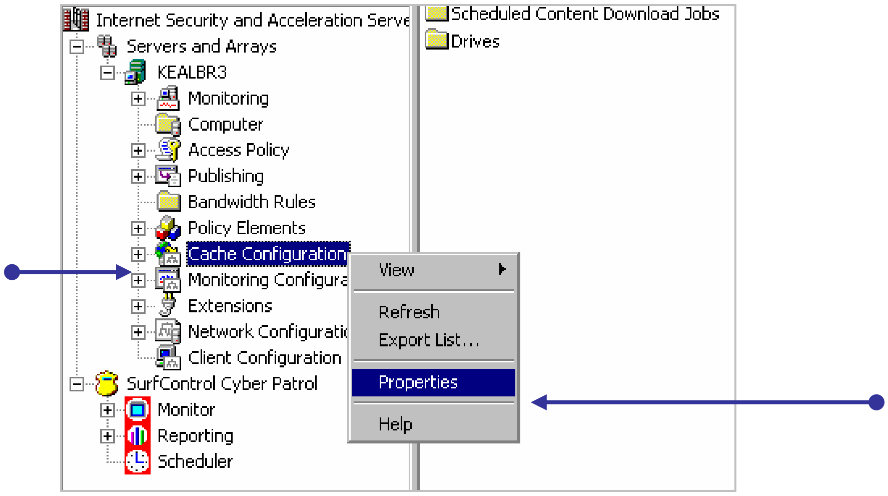
```
etest.ncs.com
etest.ncspearson.com
www1.etest.ncs.com
www1.etest.ncspearson.com
www3.etest.ncs.com
www3.etest.ncspearson.com
www4.etest.ncs.com
www4.etest.ncspearson.com
www5.etest.ncs.com
www5.etest.ncspearson.com
```

3. Click **Add URLs** to implement changes.

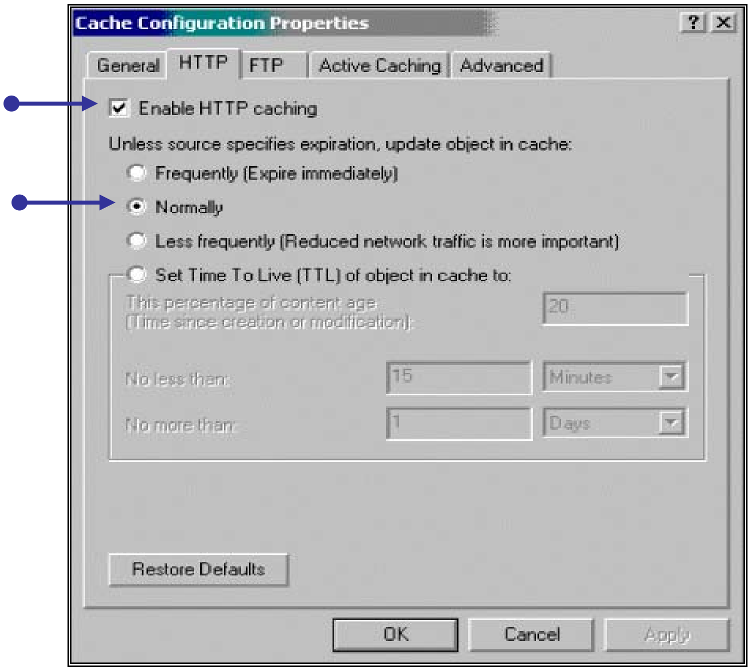
Enable HTTP Caching within Microsoft ISA Server

Enabling HTTP caching will reduce the amount of Internet bandwidth required for electronic testing. The following steps illustrate how to configure HTTP caching.

1. In the ISA Server Management Console, right click on Cache Configuration and select Properties.



2. Select the HTTP tab and enable Enable HTTP Caching by placing a check in the check box. Set the expiration to Normal.



☑ Enable HTTP caching

Unless source specifies expiration, update object in cache:

○ Frequently (Expire immediately)

● Normally

○ Less frequently (Reduced network traffic is more important)

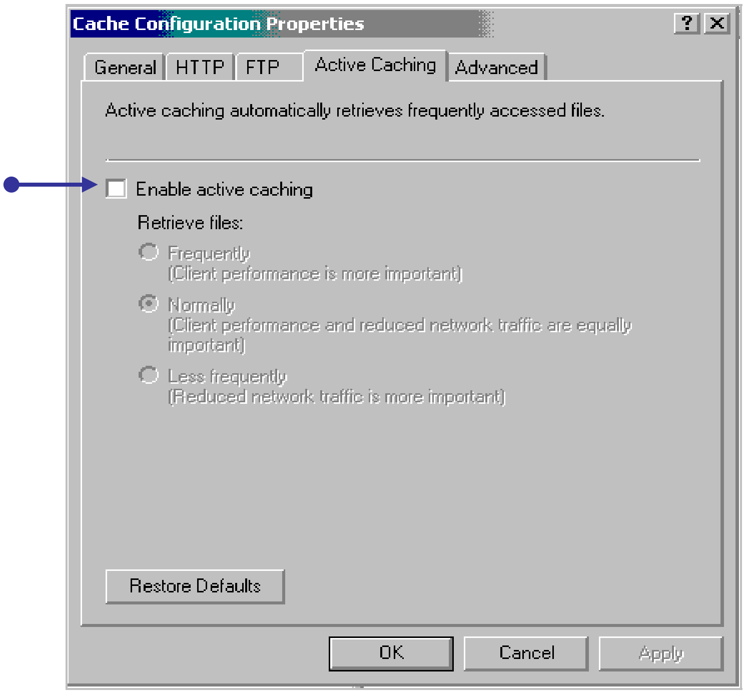
○ Set Time To Live (TTL) of object in cache to:

This percentage of content age (Time since creation or modification): 20

No less than: 15 Minutes

No more than: 1 Days

3. Select the Active Caching tab. Disable active caching by ***removing*** the check in the Enable active caching check box.



Active caching automatically retrieves frequently accessed files.

☐ Enable active caching

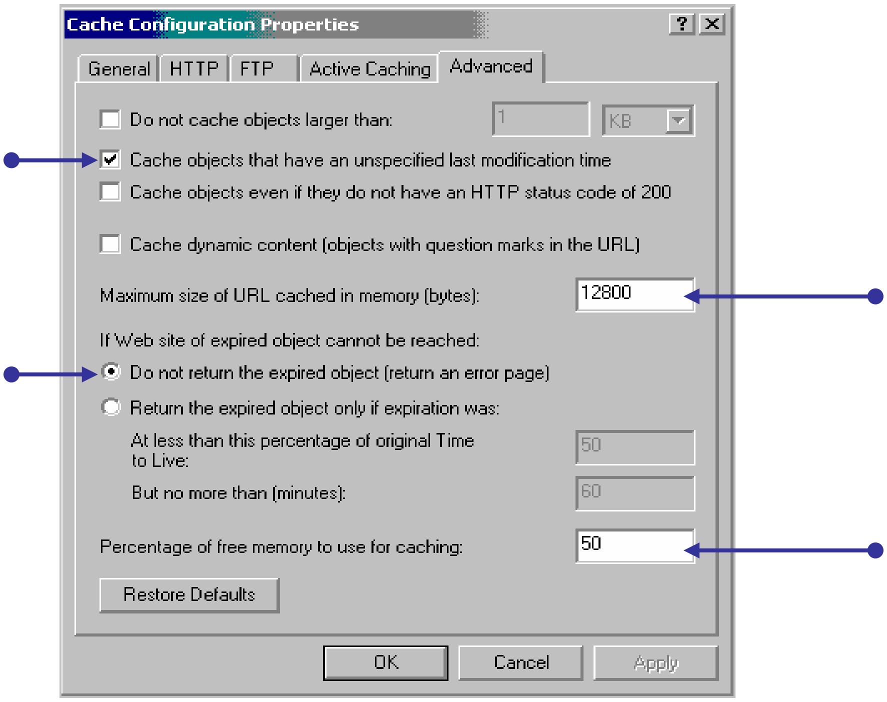
Retrieve files:

○ Frequently
(Client performance is more important)

● Normally
(Client performance and reduced network traffic are equally important)

○ Less frequently
(Reduced network traffic is more important)

4. Select the Advanced tab. Configure the Advanced options as shown below.



☐ Do not cache objects larger than: 1 KB

☑ Cache objects that have an unspecified last modification time

☐ Cache objects even if they do not have an HTTP status code of 200

☐ Cache dynamic content (objects with question marks in the URL)

Maximum size of URL cached in memory (bytes): 12800

If Web site of expired object cannot be reached:

● Do not return the expired object (return an error page)

○ Return the expired object only if expiration was:

At less than this percentage of original Time to Live: 50

But no more than (minutes): 60

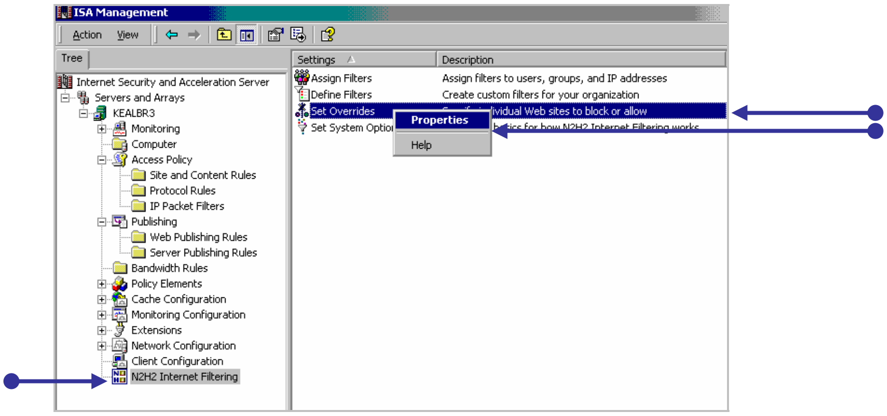
Percentage of free memory to use for caching: 50

5. Click **OK** to implement the changes.

N2H2/Microsoft ISA Server Configuration Guidelines

Set an N2H2 Override

1. In the ISA Server Management Console, select N2H2 Filtering in the Tree field, then select Set Overrides / Properties in the Settings field.

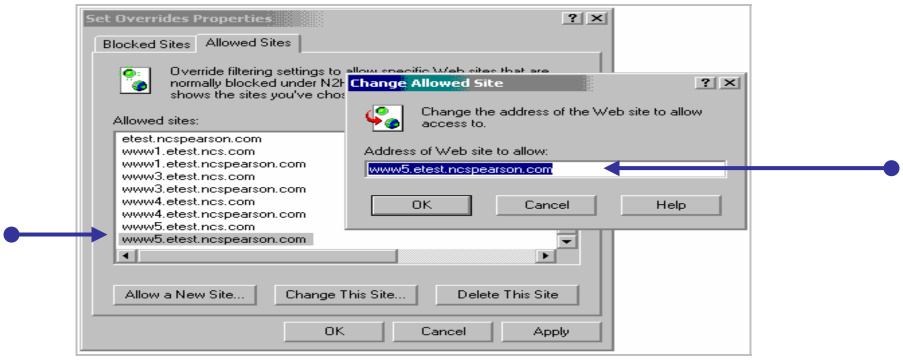


Settings	Description
Assign Filters	Assign filters to users, groups, and IP addresses
Define Filters	Create custom filters for your organization
Set Overrides	ividual Web sites to block or allow
Set System Optio	tics for how N2H2 Internet Filtering works

2. In the Set Overrides Properties screen, select the Allowed Sites tab, then click **Allow a New Site**.

3. Add the sites specified below by entering each URL one at a time into the Address of Web Site to Allow field. Then click **OK.**

etest.pearson.com
www8.etest.pearson.com
www9.etest.pearson.com
launcher.etest.pearson.com



Override filtering settings to allow specific Web sites that are normally blocked under N2H shows the sites you've chos

Allowed sites:

etest.ncspearson.com
www1.etest.ncs.com
www1.etest.ncspearson.com
www3.etest.ncs.com
www3.etest.ncspearson.com
www4.etest.ncs.com
www4.etest.ncspearson.com
www5.etest.ncs.com
www5.etest.ncspearson.com

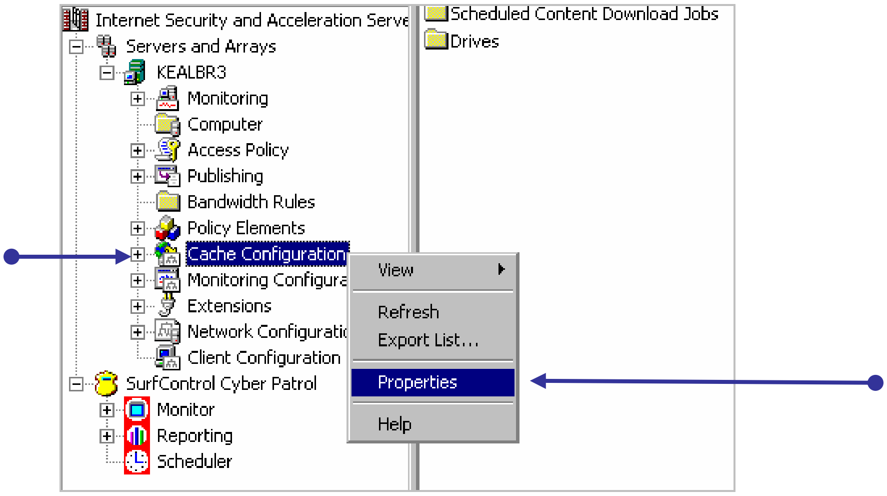
Change the address of the Web site to allow access to.

Address of Web site to allow: www5.etest.ncspearson.com

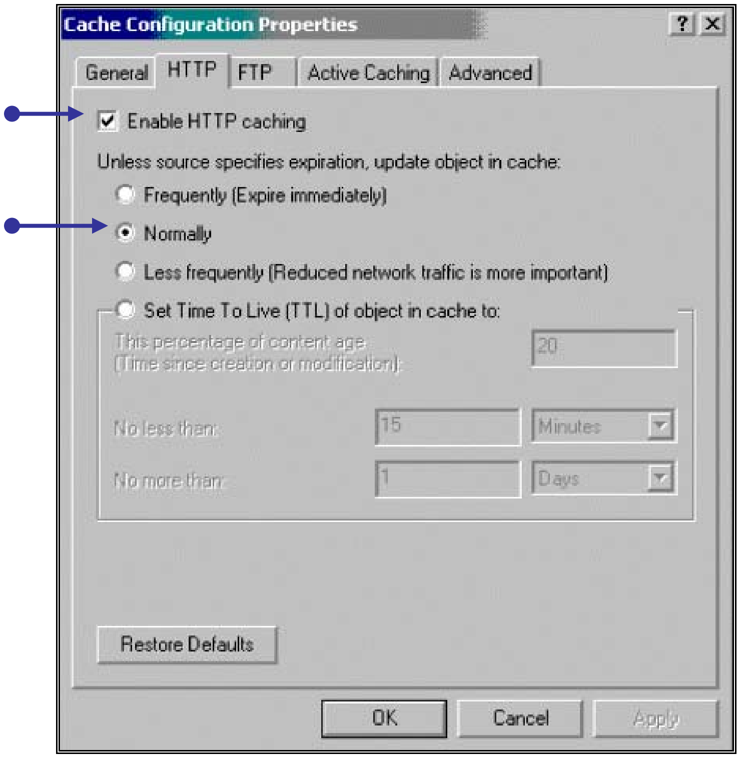
Enable HTTP Caching within Microsoft ISA Server

Enabling HTTP caching will reduce the amount of Internet bandwidth required for electronic testing. To configure HTTP caching:

1. In the ISA Server Management Console, right click on Cache Configuration and select Properties.



2. Select the HTTP tab and enable Enable HTTP Caching by placing a check in the check box. Set the expiration to Normal.


Cache Configuration Properties

General | HTTP | FTP | Active Caching | Advanced

☑ Enable HTTP caching

Unless source specifies expiration, update object in cache:

○ Frequently (Expire immediately)

● Normally

○ Less frequently (Reduced network traffic is more important)

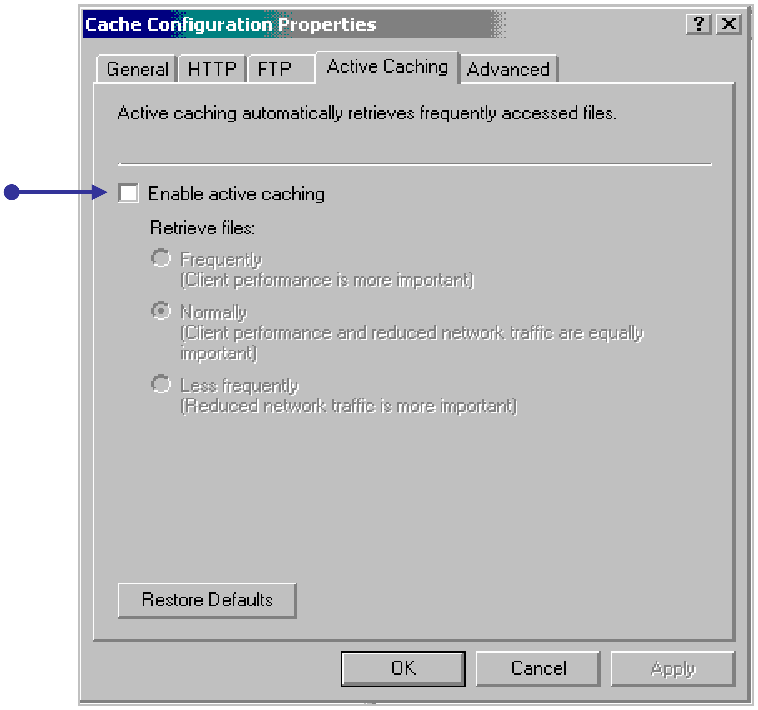
○ Set Time To Live (TTL) of object in cache to:

This percentage of content age (Time since creation or modification): 20

No less than: 15 Minutes

No more than: 1 Days

3. Select the Active Caching tab. Disable active caching by ***removing*** the check from the Enable active caching check box.



Cache Configuration Properties

Active caching automatically retrieves frequently accessed files.

□ Enable active caching

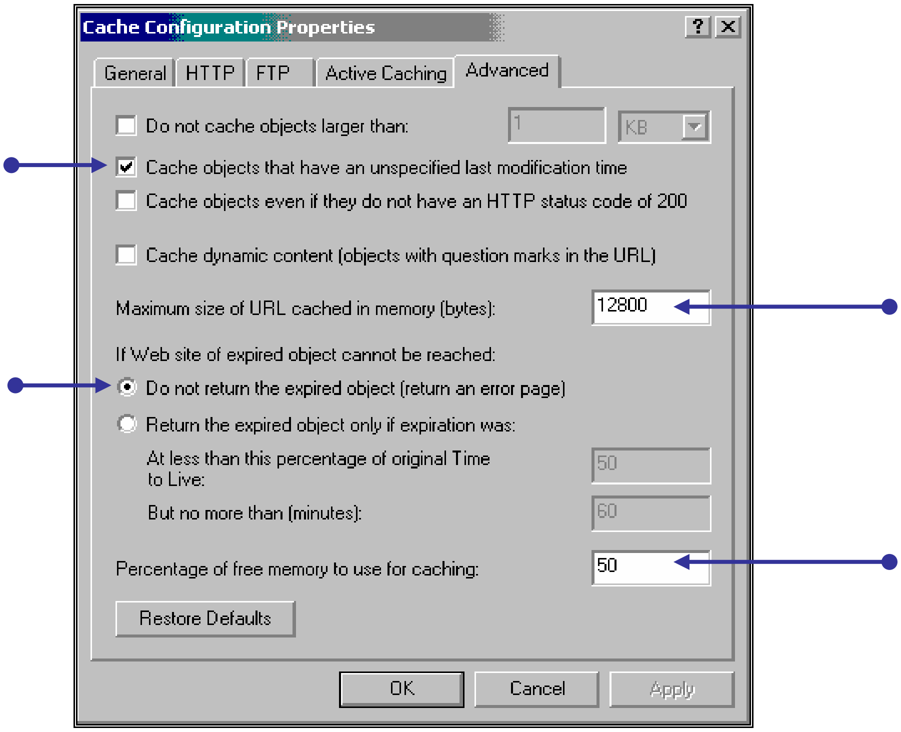
Retrieve files:

○ Frequently
(Client performance is more important)

● Normally
(Client performance and reduced network traffic are equally important)

○ Less frequently
(Reduced network traffic is more important)

4. Select the Advanced tab. Configure the Advanced options as shown below.



Cache Configuration Properties

□ Do not cache objects larger than: 1 KB

☑ Cache objects that have an unspecified last modification time

□ Cache objects even if they do not have an HTTP status code of 200

□ Cache dynamic content (objects with question marks in the URL)

Maximum size of URL cached in memory (bytes): 12800

If Web site of expired object cannot be reached:

● Do not return the expired object (return an error page)

○ Return the expired object only if expiration was:

At less than this percentage of original Time to Live: 50

But no more than (minutes): 60

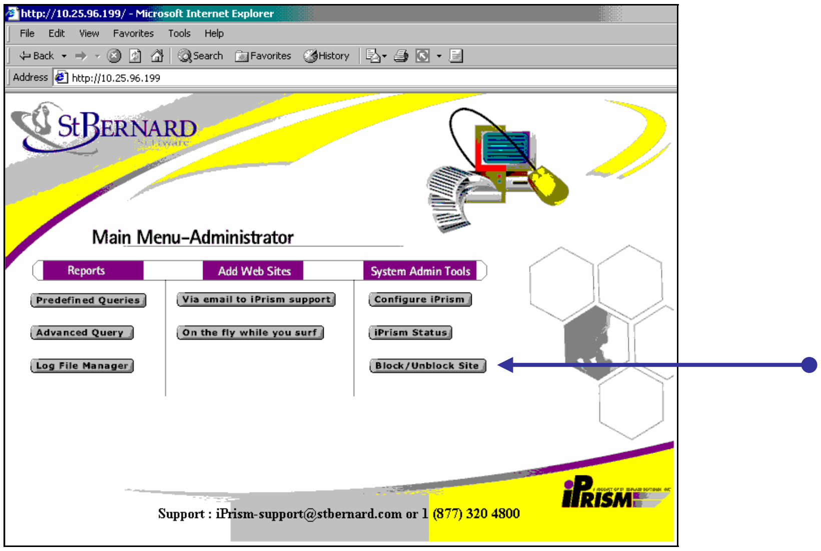
Percentage of free memory to use for caching: 50

5. Click **OK** to implement the changes.

iPrism Configuration Guidelines

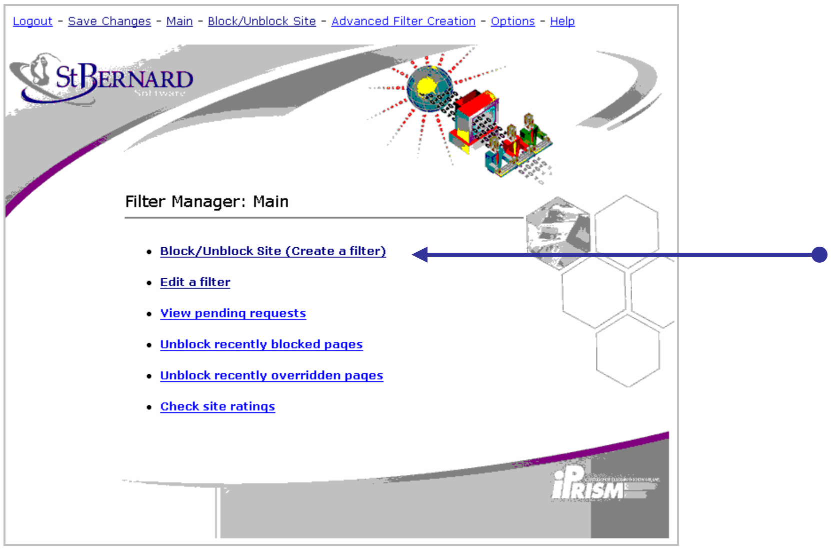
Unblock the PEMSolutions sites within iPrism

1. On the iPrism management web page, click **Block/Unblock Site**.

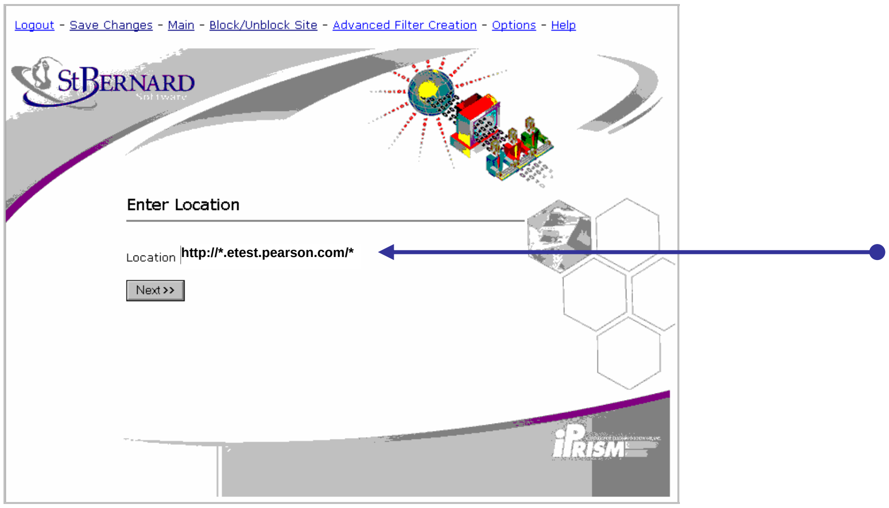

http://10.25.96.199/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.25.96.199
StBERNARD Software
Main Menu–Administrator
Reports
Add Web Sites
System Admin Tools
Predefined Queries
Advanced Query
Log File Manager
Via email to iPrism support
On the fly while you surf
Configure iPrism
iPrism Status
Block/Unblock Site
iPRISM

Support : iPrism-support@stbernard.com or 1 (877) 320 4800

2. On the Filter Manager screen, click on the **Block/Unblock Site (Create a filter)** link.


Logout - Save Changes - Main - Block/Unblock Site - Advanced Filter Creation - Options - Help
StBERNARD Software
Filter Manager: Main
Block/Unblock Site (Create a filter)
Edit a filter
View pending requests
Unblock recently blocked pages
Unblock recently overridden pages
Check site ratings
iPRISM

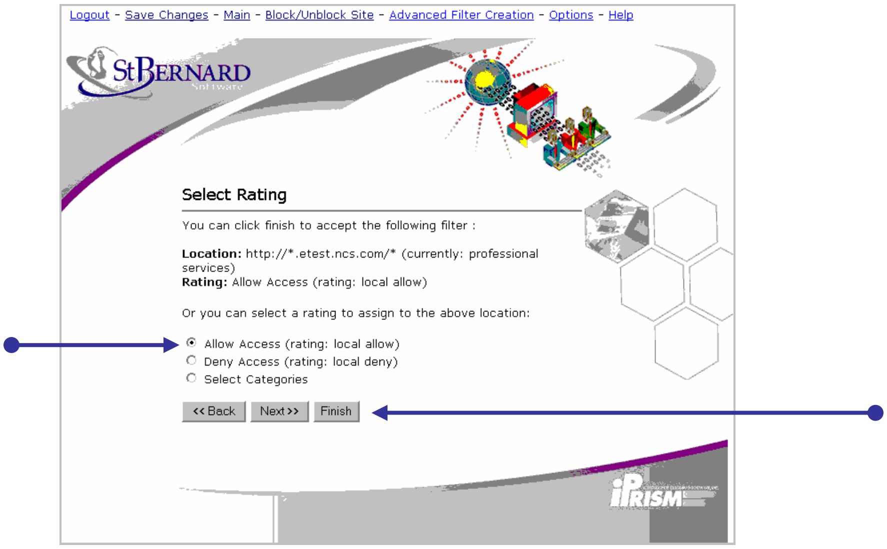
3. On the Enter Location screen, enter **http://*.etest.pearson.com/*** in the Location field, then click **Next**.


Logout - Save Changes - Main - Block/Unblock Site - Advanced Filter Creation - Options - Help
StBERNARD Software
Next >>
iPRISM

Enter Location

Location http://*.etest.pearson.com/*

4. On the Select Rating Screen, select Allow Access (rating: local allow), then click **Finish.**


Logout - Save Changes - Main - Block/Unblock Site - Advanced Filter Creation - Options - Help
StBERNARD Software
<< Back
Next >>
Finish
iPRISM

Select Rating

You can click finish to accept the following filter :

Location: http://*.etest.ncs.com/* (currently: professional services)
Rating: Allow Access (rating: local allow)

Or you can select a rating to assign to the above location:

● Allow Access (rating: local allow)
○ Deny Access (rating: local deny)
○ Select Categories

Caching with iPrism

The iPrism device does not provide a caching function. Implementing a separate cache server in addition to iPrism can greatly decrease the download times for PEMSolutions while also reducing the load placed on your network and Internet connection.